

What Nanoheal collects, where it lives, and your GDPR position.

The Nanoheal agent reads how each device and its apps are performing, so IT can find problems and fix them. This sheet lists the kinds of data it collects and why, where that data is kept, and who is responsible for it under the GDPR.

What the agent collects

In short: device health, applications, network, call quality, policy state, identity, survey answers and the record of each automation run.

KIND OF DATA	FOR EXAMPLE	USED FOR
Device health	Boot and logon time, CPU, memory, disk, battery health, OS and build	The experience score, forecasts, slow-device alerts
Applications	Installed software and versions, how apps are used, crashes and hangs	Crash analysis, patching and licence work
Network	Wi-Fi and VPN quality, latency to the services people use, web response times	Network and web experience
Calls	Teams call quality: jitter, packet loss, freezes	Call-quality reporting
Policy and events	Windows events, the device's state against your policies	Compliance and drift correction
Identity	Device name, user and device identifiers, department, group and site	Cutting results by team or site
Sentiment	Answers employees give in pulse surveys	The sentiment half of the experience score
Automation runs	What ran, when, on which device, the result and the check after	The audit log, before-and-after reporting

What it does not collect

Sensitive information such as credit card numbers, IBANs or social security numbers. Nor the contents of files, email or chats, keystrokes, or screen recordings.

You set the limits

What is collected, who can see it, whether it is anonymised and how long it is kept follow your configuration. Collection of identifiers such as serial numbers can be switched off on the server. Haya masks the fields you declare as personal.

Your GDPR position

Who is responsible

You are the controller of the data the platform collects about your employees. Nanoheal processes it on your instructions, under a data processing agreement.

Where it lives

The SaaS runs on AWS by default, with Azure and GCP customer environments also supported, in the region set for your deployment. On-premises and air-gapped deployments are designed with your team.

Requests from employees

As controller you answer them, and we help. Deletion requests to us go to **privacy@nanoheal.com**.

The paperwork

A data processing agreement on request, with the sub-processor list that applies to your deployment.

How long it is kept

Retention and deletion are agreed with each customer, by deployment and contract.

If something goes wrong

We follow the SANS incident process and tell affected customers as soon as possible, by email and phone, with updates until it is closed.

How it is protected

- Encrypted at rest with AWS Key Management Service, and in transit with TLS; mutual TLS between client and server.
- Role-based access, approvals before fixes run, and a log of who did what.
- Haya, Nanoheal's AI and analytics, runs behind approval gates, role-based access, execution traces and PII masking, on your choice of model, including a locally hosted one.
- SOC 2 Type I, SOC 2 Type II in progress, and GDPR. The SOC 2 report on request.

For your review. Request the DPA, the SOC 2 report or field-level collector detail at nanoheal.com/demo/security, or write to **security@nanoheal.com**.